Alexander A. Baehr, WSBA #25320
SUMMIT LAW GROUP, PLLC
315 Fifth Avenue S, Suite 1000
Seattle, WA 98104
Telephone: (206) 676-7000

Ekwan E. Rhow (pro hac vice forthcoming)
Marc E. Masters (pro hac vice forthcoming)
Barr Benyamin (pro hac vice forthcoming)
BIRD, MARELLA, BOXER, WOLPERT, NESSIM, DROOKS, LINCENBERG & RHOW, P.C.
1875 Century Park East, 23rd Floor
Los Angeles, California 90067
Telephone: (310) 201-2100

Jonathan M. Rotter (pro hac vice forthcoming)
Kara M. Wolke (pro hac vice forthcoming)
Pavithra Rajesh (pro hac vice forthcoming)
GLANCY PRONGAY & MURRAY LLP
1925 Century Park East, Suite 2100
Los Angeles, California 90067
Telephone: (310) 201-9150

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON

JANE DOE, Individually and on Behalf of All Others Similarly Situated,

Plaintiff,

v.

MICROSOFT CORPORATION, a Washington Corporation; QUALTRICS INTERNATIONAL INC., a Delaware Corporation; and QUALTRICS LLC, a Delaware Limited Liability Company,

Defendants.

Case No. 2:23-cv-718

COMPLAINT – CLASS ACTION

DEMAND FOR JURY TRIAL

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone: (206) 676-7000
Fax: (206) 676-7001

Plaintiff Jane Doe ("Plaintiff"), individually and on behalf of all others similarly situated, for her complaint against Microsoft Corporation, Qualtrics International, Inc., and Qualtrics LLC (together, "Defendants") alleges the following upon information and belief, except as to those allegations concerning Plaintiff, which are alleged upon personal knowledge.

I. NATURE AND OVERVIEW OF THE ACTION

1. Patients rightfully expect that their healthcare will be private. And the law protects the privacy of healthcare information. This case is about a serious violation of that core privacy interest.

2. Plaintiff, like millions of other class members, obtains healthcare from Kaiser Permanente ("Kaiser"). As is true for any medical provider, the law protects the privacy of the healthcare information held by Kaiser and exchanged between Plaintiff and Class Members, on the one hand, and Kaiser, on the other.

3. One place that legal protection is important is the Kaiser Website, which Kaiser Members use to access their medical records, including prescriptions and immunizations, research their medical conditions, find and communicate with doctors, and undertake other interactions related to the provision of healthcare services.

4. Unfortunately and unlawfully, Defendants repeatedly and systematically have violated that legally-protected privacy interest by extracting private healthcare and other information from Kaiser Members' communications with the Kaiser Website.

5. Through Defendants' code implemented on the Kaiser Website, Defendants have vacuumed up information about Kaiser Members' medical conditions, immunizations, prescriptions, physician information, and other private data, including healthcare search terms, videos watched, and links accessed. And all of that information is linked to particular patients because Defendants each take that data together with unique identifiers that allow Defendants to identify the Kaiser Member.

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone: (206) 676-7000
Fax: (206) 676-7001

6. Plaintiff and class members did not consent to Defendants' taking this highly sensitive and legally-protected medical and other information. Defendants' conduct is unlawful, and it must be stopped.

II. PARTIES

7. Plaintiff Jane Doe is a resident of California. She is suing as a Jane Doe because the confidentiality of her patient status is protected by law, as explained below. She has been a Kaiser Member for at least 10 years and has used the Kaiser Website throughout her membership. She has an account on the Kaiser Website. While logged into that account, she used the search function; accessed immunization and medical records; made appointments; reviewed physician information; reviewed medical conditions; and watched videos. As more fully explained below, Defendants unlawfully intercepted and collected such data along with her personal identifiers.

8. Defendant Microsoft Corporation ("Microsoft") is a publicly traded company incorporated under the laws of Washington with its principal executive offices located in Redmond, Washington. Microsoft offers computer hardware and software products for business and personal users, including data analytics and cloud-computing applications. Among Microsoft's various business segments is its Search and News Advertising Business, which "is designed to deliver relevant search, native, and display advertising to a global audience."[1]

9. Defendant Qualtrics International, Inc. is a Delaware corporation, and Defendant Qualtrics LLC is a Delaware limited liability company ("Qualtrics"). Qualtrics' principal places of business are located in Seattle, Washington and in Provo, Utah. Qualtrics offers a cloud-based subscription software platform for "experience management" for other organizations.

III. JURISDICTION AND VENUE

10. The Court has personal jurisdiction over Defendants because they each have sufficient minimum contacts with this District in that each Defendant operates and markets its

[1] Microsoft, Form 10-K for the period ended June 30, 2022 at 15 (July 28, 2022), https://www.sec.gov/ix?doc=/Archives/edgar/data/0000789019/000156459022026876/msft-10k_20220630.htm

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone: (206) 676-7000
Fax: (206) 676-7001

services throughout this State. Additionally, Defendants Microsoft and Qualtrics are headquartered in this District.

11. This Court has subject matter jurisdiction pursuant to the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, *et seq.* The Court has supplemental jurisdiction over the remaining state law claims pursuant to 28 U.S.C. § 1367 because the state law claims form part of the same case or controversy.

12. The Court also has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2) because the amount in controversy exceeds $5 million, exclusive of interest and costs, and Plaintiff is diverse from each Defendant.

13. Venue is proper in this District because a substantial part of the events or omissions giving rise to the claim occurred in this District. Specifically, Defendants' principal executive offices are located in this District.

IV. SUBSTANTIVE ALLEGATIONS

A. The Health Insurance Portability and Accountability Act ("HIPAA")

14. Patient health care information in the United States is protected by federal law under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its implementing regulations promulgated by the United States Department of Health and Human Services ("HHS").

15. The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other individually identifiable health information (collectively defined as "protected health information" or "PHI") and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of protected health information and sets limits and conditions on the uses and disclosures that may be made of such information without an individual's authorization. The Rule also gives individuals rights over their protected health information, including rights to examine and obtain a copy of their health records, to direct a covered entity to transmit to a third party an electronic copy of their protected health information in an

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone: (206) 676-7000
Fax: (206) 676-7001

electronic health record, and to request corrections. The Privacy Rule is located at 45 CFR Part 160 and Subparts A and E of Part 164. https://www.hhs.gov/hipaa/forprofessionals/privacy/index.html.

16. Under 45 C.F.R. § 164.502, a health care provider or business associate of a health care provider "may not use or disclose 'protected health information' except as permitted or required by" the HIPAA Privacy Rule.

17. Under 45 C.F.R. 160.103, the Privacy Rule defines "protected health information" or PHI as "individually identifiable health information" that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium."

18. Under 45 C.F.R. § 160.103, the Privacy Rule defines "individually identifiable health information" as "a subset of health information, including demographic information collected from an individual" that is (1) "created or received by a health care provider;" (2) "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;" and (3) either (a) identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual."

19. Under 45 C.F.R. § 164.514, the HIPAA de-identification rule states that "health information is not individually identifiable only if" (1) an expert "determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information" and "documents the methods and results of the analysis that justify such determination'" or (2) "the following identifiers of the individual or of relatives, employers, or household members of the individual are removed: Names … Medical record numbers; … Account numbers … Device identifiers and serial numbers; … Web Universal Resource Locators (URLs); Internet Protocol (IP) address numbers; … and any other unique identifying number, characteristic, or code." In addition, the covered entity must not "have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information."

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone: (206) 676-7000
Fax: (206) 676-7001

20. Under 42 U.S.C. § 1320d-6, any "person [individual … or a corporation] who knowingly and in violation of this part—(1) uses or causes to be used a unique health identifiers; [or] (2) obtains individually identifiable health information relating to an individual … shall be punished" by fine or, in certain circumstances, imprisonment, with increased penalties for "intent to sell, transfer, or use individually identifiable health information for commercial advantage[.]" The statute further provides that a "person … shall be considered to have obtained or disclosed individually identifiable health information … if the information is maintained by a covered entity … and the individual obtained or disclosed such information without authorization."

21. Patient status (i.e., information connecting an individual with a healthcare provider) alone is protected by HIPAA. See In re Meta Pixel Healthcare Lit., 2022 U.S. Dist. LEXIS 230754, *27-28 (N.D. Cal. Dec. 22, 2022) (holding that patient status is protected information under HIPAA); Arvidson v. Buchar, No. ST-16-cv-410, 2018 WL 10613032, at *10 (V.I. Super. Ct. June 6, 2018) (ruling that patient names and a patient list were PHI which were therefore subject to special disclosure requirements under HIPAA); Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates, U.S. Health & Human Services (HHS guidance instructing that information which connect an individual with a healthcare provider "is indicative that the individual has received or will receive health care services," and thus "relates to the individual's past, present, or future health or health care or payment for care") (content current as of [*28] Dec. 1, 2022), https://www.hhs.gov/hipaa/forprofessionals/privacy/guidance/hipaa-onlinetracking/ index.html.

22. Guidance from HHS instructs health care providers that patient status is protected by HIPAA. In Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act Privacy Rule, HHS sets out:

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data.

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone: (206) 676-7000
Fax: (206) 676-7001

> *… If such information was listed with health condition, health care provision or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.*[2]

23. In its guidance for Marketing, HHS further instructs:

> The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. … Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, *covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list.*[3]

24. HHS has previously instructed that HIPAA covers patient-status alone:

(a) "The sale of a patient list to a marketing firm" is not permitted under HIPAA. 65 Fed. Reg. 82717 (Dec. 28, 2000);

(b) "A covered entity must have the individual's prior written authorization to use or disclose protected health information for marketing communications," which would include disclosure of mere patient status through a patient list. 67 Fed. Reg. 53186 (Aug. 14, 2002);

(c) It would be a HIPAA violation "if a covered entity impermissibly disclosed a list of patient names, addresses, and hospital identification numbers." 78 Fed. Reg. 5642 (Jan. 25, 2013); and

(d) The only exception permitting a hospital to identify patient status without express written authorization is to "maintain a directory of individuals in its facility" that includes name, location, general condition, and religious

[2] https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/Deidentification/hhs_deid_guidance.pdf at 5 (emphasis added).

[3] https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf at 1-2 (emphasis added).

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone: (206) 676-7000
Fax: (206) 676-7001

affiliation when used or disclosed to "members of the clergy" or "other persons who ask for the individual by name." 45 C.F.R. § 164.510(1). Even then, patients must be provided an opportunity to object to the disclosure of the fact that they are a patient. 45 C.F.R. § 164.510(2).

25. There is no HIPAA-exception for the Internet or online patient portals.

26. Plaintiff, Class Members, and Subclass Members have not given consent to Defendants' possession or use of Plaintiff, Class Members, and Subclass Members' PHI.

27. More broadly, even outside the HIPAA context, there is no consent to a third party intercepting and collecting one's private information data unless the individual understands that she is authorizing the third party to collect such private medical information. And the third party must expressly and specifically disclose that it may acquire the individual's *medical information* and not just the individual's information in a general sense. *See In re Meta Pixel Healthcare Lit.*, --- F. Supp. 3d. ---, 2022 U.S. Dist. LEXIS 230754, *30-31 (N.D. Cal. Dec. 22, 2022) (holding that plaintiffs did not consent to Meta's collection of their medical information where Meta's policies did not "specifically indicate that Meta may acquire *health data* obtained from Facebook users' interactions with their *medical providers'* websites," since "[Meta's] generalized notice is not sufficient to establish consent").

B. Background on Kaiser and its Website

28. Third-party Kaiser Permanente ("Kaiser") is an integrated managed care consortium of for-profit and non-profit entities that is headquartered in Oakland, California. It operates 39 hospitals across eight states (California, Washington, Oregon, Colorado, Hawaii, Georgia, Maryland, and Virginia).[4] Kaiser serves a total of 12.6 million members, and approximately 9.4 million of them (or roughly 75%) reside in California.

[4] https://about.kaiserpermanente.org/who-we-are/fast-facts

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone: (206) 676-7000
Fax: (206) 676-7001

29. Kaiser operates a website at https://healthy.kaiserpermanente.org/ (the "Kaiser Website") through which it communicates with its members ("Kaiser Members") and non-members who use the Kaiser Website. By logging into their individual patient portal ("Kaiser Account"), Kaiser Members can make appointments, search for doctors, review and manage their prescriptions, and review their medical records and medical history more broadly.

30. Unbeknownst to Kaiser Members, code on the Kaiser Website includes software development kits ("SDKs") offered by Defendants Microsoft and Qualtrics that intercept and collect Kaiser Members' activity and their private medical data. These SDKs intercept and collect search terms, videos watched, and the URLs of links that are accessed, all of which are associated with unique user identifiers that are collected and enable each Defendant to identify the Kaiser Member associated with the data. The Defendants' SDKs covertly employ their tracking code such that Kaiser Members have no indication that their web activity is transmitted to Defendants.

31. None of the Defendants' SDKs are necessary for medically services.

C. Each of the Defendants' SDKs Collects Personal Data, PII, and PHI from Kaiser Members

32. Each of the Defendants' SDKs collects a vast array of user data and content based on a user's browsing activity on the Kaiser Website, including a user's personally identifiable information ("PII"), a user's PHI, a user's search terms entered in the Kaiser Website, the URLs of each page on the Kaiser Website that a user navigates to and/or from, the videos on the Kaiser Website a user views, and/or the unique user identifiers a particular SDK associates with a user (collectively, "Private Data").

1. Microsoft

33. The Kaiser Website code includes Microsoft's SDK (the "Microsoft SDK"). The Microsoft SDK is tracking software that collects a user's internet data through several unique user identifiers and cookies. The unique user identifiers and cookies that the Microsoft SDK utilizes to

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone: (206) 676-7000
Fax: (206) 676-7001

collect a user's data include the user's: (i) Microsoft Machine Unique Identifier ("MUID"); (ii) Windows Live ID ("WLID"); and (iii) and the user's WLS identifier ("WLS").

34. The MUID cookie is a unique user identifier used for advertising, site analytics, and other operational purposes, which links the user data it collects to a specific user and consists of an alphanumeric string.

35. The WLID is a unique user identifier assigned to a specific user that consists of an alphanumeric string and the user's name.

36. The WLS is a unique user identifier assigned to a specific user that consists of an alphanumeric string. The WLS also includes a user's real name.

37. The Microsoft SDK also collects and sends to Microsoft identifying information about a user's web browser, which it collectively terms "User-Agent" ("User Agent Data").

38. As integrated into the Kaiser Website, the Microsoft SDK intercepts and collects a plethora of Private Data, including PII and PHI, from Kaiser Members when they use the Kaiser Website without their knowledge or consent. The Private Data intercepted and collected includes, as further described herein, search queries, visited webpages, videos, prescriptions, medical conditions, immunization records, and allergies.

39. **Search Queries**: The Kaiser Website contains an integrated search bar that allows visitors to the Kaiser Website to search for information on Kaiser's Website using search terms, similar to using an Internet search engine like Google or Yahoo. Whenever a user on Kaiser's Website utilizes the search bar on Kaiser's Website to search for information, the Microsoft SDK intercepts and collects the search terms entered by the user, along with unique user identifiers associated with the user, including MUID, WLID, and WLS. The unique user identifiers allow Microsoft to link the search terms to a specific Kaiser Website user and identify the Kaiser Website user. Microsoft's ability to identify the Kaiser Website user is enhanced by the SDK's collection of User Agent Data.

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone: (206) 676-7000
Fax: (206) 676-7001

40. The Microsoft SDK intercepts and collects all search queries, without discerning their sensitivity, including, for example, those related to specific medical conditions a Kaiser Website user is afflicted with, symptoms a Kaiser Website user is experiencing, or medications a Kaiser Website user is prescribed.

41. Kaiser Website users, including Plaintiff and the Class Members, are unaware that Microsoft is intercepting and collecting the above-described data through its SDK, and have not provided their consent, whether implied or express, for Microsoft to obtain this data.

42. **Visited Webpages**: The Microsoft SDK intercepts and collects the URL (*i.e.,* web address) and/or title of each page on the Kaiser Website that a Kaiser Website user navigates to, the URL of the webpage from which the Kaiser Website user navigated to the newly-visited page, and the unique user identifiers associated with the Kaiser Website user, including MUID, WLID, and WLS. The unique user identifiers allow Microsoft to link the visited webpage to a specific Kaiser Website user and identify that Kaiser Website user. Microsoft's ability to identify the Kaiser Website user is enhanced by the SDK's collection of User Agent Data. The collection of a Kaiser Website user's visited URLs and/or their titles occurs regardless of whether the Kaiser Website user is logged into her Kaiser Account.

43. Furthermore, as explained below, when a Kaiser Member is logged into her Kaiser Account through the Kaiser Website, the collected URLs and webpage titles divulge to Microsoft some or all of the Kaiser Member's medical history and PHI, including the medications the Kaiser Member is prescribed, the medical conditions the Kaiser Member suffers from, the Kaiser Member's immunization record, and the Kaiser Member's allergies. Such URLs and page titles, when linked with unique user identifiers such as MUID, WLID, and WLS, allow Microsoft to link medical information, including PHI, to individual Kaiser Members.

44. Kaiser Website users, including Kaiser Members accessing their Kaiser Accounts through the Kaiser Website, such as Plaintiff and the Class Members, are unaware that Microsoft is

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone: (206) 676-7000
Fax: (206) 676-7001

collecting the above-described data through its SDK, and have not provided their consent, whether implied or express, for Microsoft to obtain this data.

45. **Videos**: The Kaiser Website contains various videos that are available for Kaiser Website users to watch. When a Kaiser Website user accesses a video on the Kaiser Website, the Microsoft SDK intercepts and collects the URL of the webpage on which the video appears and the title of the video, along with unique user identifiers associated with the Kaiser Website user, including MUID, WLID, and WLS. The unique user identifiers allow Microsoft to link the accessed video to a specific Kaiser Website user and identify the Kaiser Website user. Microsoft's ability to identify the Kaiser Website user is enhanced by the SDK's collection of User Agent Data. The collection and transfer of data relating to videos on the Kaiser Website occurs regardless of whether the Kaiser Website user is logged in to her Kaiser Account.

46. Kaiser Website users, including Plaintiff and the Class Members, are unaware that Microsoft is collecting the above-described data through its SDK, and have not provided their consent, whether implied or express, for Microsoft to obtain this data.

47. **Prescriptions**: When logged in to her Kaiser Account on the Kaiser Website, a Kaiser Member is able to view each of her prescribed medications by navigating to her personalized "Prescription Details" page. When viewing her list of medications, a Kaiser Member is able to click on a medication to navigate to a webpage within Kaiser's "Drug encyclopedia" with additional information about that medication in order to learn more about it. Unbeknownst to Kaiser Members, when a Kaiser Member clicks on a medication and navigates to that medication's "Drug encyclopedia" webpage, the Microsoft SDK intercepts and collects: (i) the URL of that page, which includes the medication's reference number in Kaiser's "Drug encyclopedia" and sometimes the medication's name; (ii) the title of that page, which includes the medication's name; (iii) the URL of the page from which the Kaiser Member is navigating (*i.e.*, the Kaiser Member's personalized "Prescription Details" page accessed from her Kaiser Account); and (iv) the Kaiser Member's MUID, WLID and/or WLS. The unique user identifiers allow Microsoft to link the prescribed

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone: (206) 676-7000
Fax: (206) 676-7001

medication to a specific Kaiser Member and identify the Kaiser Member. Microsoft's ability to identify the Kaiser Member is enhanced by the SDK's collection of User Agent Data. Additionally, since the Microsoft SDK also intercepts and collects the URL from which the Kaiser Member is navigating—the Kaiser Member's personalized "Prescription Details" page, which is only accessible when the Kaiser Member logs in to her Kaiser Account—Microsoft is able to determine that the individual is, in fact, a Kaiser Member, and that the medication is prescribed to the Kaiser Member.

48. The above-described data is PHI, since it is individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.

49. Kaiser Members, including Plaintiff and the Class Members, are unaware that Microsoft is collecting the above-described data through its SDK, and have not provided their consent, whether implied or express, for Microsoft to obtain this data.

50. **Medical Conditions**: When logged in to her Kaiser Account through the Kaiser Website, a Kaiser Member is able to view each of her medical conditions by navigating to her personalized "Medical Record" page and then further navigating to her personalized "Health summary" page. When viewing her list of medical conditions, each listed condition contains a hyperlink reading "Learn more" that, when clicked, automatically runs a search on the Kaiser Website for that medical condition using the name of the condition as a search query and navigates the Kaiser Member to a webpage on the Kaiser Website containing the search results. Unbeknownst to Kaiser Members, when a Kaiser Member clicks on the "Learn more" hyperlink for a given medical condition, the Microsoft SDK intercepts and collects: (i) the URL of the page containing the search results, which contains the name of the medical condition used for the search query and reveals that the user navigated from her personalized "Health Summary" subpage within her "Medical Record" page accessed from her Kaiser Account; (ii) the title of the page containing the search results, which identifies that the Kaiser Member navigated from her personalized "Medical

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone: (206) 676-7000
Fax: (206) 676-7001

Record" page; and (iii) the Kaiser Member's MUID, WLID and/or WLS. The unique user identifiers allow Microsoft to link the medical condition to a specific Kaiser Member and identify the Kaiser Member. Microsoft's ability to identify the Kaiser Member is enhanced by the SDK's collection of User Agent Data. Additionally, since the Microsoft SDK also intercepts and collects data revealing the page from which the Kaiser Member is navigating—the Kaiser Member's personalized "Health summary" page, which is only accessible when the Kaiser Member logs in to her Kaiser Account—as well as data showing that the Kaiser Member accessed the page containing the search results from her personal "Medical Record" page more generally, Microsoft is aware that the individual is a Kaiser Member and that the Kaiser Member suffers from the medical condition.

51. The above-described data is PHI, since it is individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.

52. Kaiser Members, including Plaintiff and the Class Members, are unaware that Microsoft is collecting the above-described data through the SDK, and have not provided their consent, whether implied or express, for Microsoft to obtain this data.

53. **Immunization Record**: When logged in to her Kaiser Account through the Kaiser Website, a Kaiser Member is able to view each of her immunizations by navigating to her personalized "Medical Record" page, from there navigating to her personalized "Health summary" page, and then selecting the "Immunizations" tab. When viewing her list of immunizations, each listed immunization contains a hyperlink reading "Learn more" that, when clicked, automatically runs a search on the Kaiser Website for the immunization using the name of the immunization as a search query and navigates the Kaiser Member to a webpage on the Kaiser Website containing the search results. Unbeknownst to Kaiser Members, when a Kaiser Member clicks on the "Learn more" hyperlink for a given immunization, the Microsoft SDK intercepts and collects: (i) the URL of the page containing the search results, which contains the name of the immunization used for the search query and reveals that the user navigated from her personalized "Medical Record" page

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone: (206) 676-7000
Fax: (206) 676-7001

accessed from her Kaiser Account; (ii) the title of the page containing the search results, which identifies that the Kaiser Member navigated from her personalized "Medical Record" page; (iii) the URL of the specific subpage within her "Medical Record" page from which the Kaiser Member is navigating (*i.e.*, the Kaiser Member's personalized "Immunizations" page); and (iv) the Kaiser Member's MUID, WLID and/or WLS. The unique user identifiers allow Microsoft to link the immunization to a specific Kaiser Member and identify the Kaiser Member. Microsoft's ability to identify the Kaiser Member is enhanced by the SDK's collection of User Agent Data. Additionally, since the Microsoft SDK intercepts and collects the specific URL from which the Kaiser Member is navigating—the Kaiser Member's personalized "Immunizations" page, which is only accessible when the Kaiser Member logs in to her Kaiser Account—as well as data showing that the Kaiser Member accessed the page containing the search results from her personal "Medical Record" page more generally, Microsoft is able to determine that the individual is a Kaiser Member and that the Kaiser Member has received the immunization.

54. The above-described data is PHI, since it is individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.

55. Kaiser Members, including Plaintiff and the Class Members, are unaware that Microsoft is collecting the above-described data through the SDK, and have not provided their consent, whether implied or express, for Microsoft to obtain this data.

56. **Allergies**: When logged in to her Kaiser Account on the Kaiser Website, a Kaiser Member is able to view each of her allergies by navigating to her personalized "Medical Record" page, from there navigating to her personalized "Health summary" page, and then selecting the "Allergies" tab. When viewing her list of allergies, each listed allergy contains a hyperlink reading "Learn more" that, when clicked, automatically runs a search on the Kaiser Website for the allergy using the name of the allergy as a search query and navigates the Kaiser Member to a webpage on the Kaiser Website containing the search results. Unbeknownst to Kaiser Members, when a Kaiser

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone: (206) 676-7000
Fax: (206) 676-7001

Member clicks on the "Learn more" hyperlink for a given allergy, the Microsoft SDK intercepts and collects: (i) the URL of the page containing the search results, which contains the name of the allergy used for the search query and reveals that the user navigated from her personalized "Medical Record" page accessed from her Kaiser Account; (ii) the title of the page containing the search results, which identifies that the Kaiser Member navigated from her personalized "Medical Record" page; and (iii) the Kaiser Member's MUID, WLID and/or WLS. The unique user identifiers allow Microsoft to link the allergy to a specific Kaiser Member and identify the Kaiser Member. Microsoft's ability to identify the Kaiser Member is enhanced by the SDK's collection of User Agent Data. Additionally, since the Microsoft SDK also intercepts and collects data showing that the Kaiser Member accessed the page containing the search results from her personal "Medical Record" page, Microsoft is able to determine that the individual is a Kaiser Member and that the Kaiser Member suffers from the allergy.

57. The above-described data is PHI, since it is individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.

58. Kaiser Members, including Plaintiff and the Class Members, are unaware that Microsoft is collecting the above-described data through the SDK, and have not provided their consent, whether implied or express, for Microsoft to obtain this data.

59. Microsoft is knowingly and intentionally intercepting and collecting, through the SDK, the above-identified data from users of the Kaiser Website, including PHI from Kaiser Members who access their Kaiser Account.

2. Qualtrics

60. Kaiser incorporates into the Kaiser Website Qualtrics' Experience Management Site Intercept software ("Site Intercept"). Site Intercept is a tracking software that collects a user's internet data through several unique user identifiers and cookies. The unique user identifiers and

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone: (206) 676-7000
Fax: (206) 676-7001

cookies that Site Intercept utilizes to collect a user's data include the user's: (i) Anonymous Survey ID ("ASID"); (ii) Contact ID; and (iii) Survey Instance ID ("SIID").

61. The ASID is a unique user identifier assigned to a specific user that consists of a numeric string.

62. The CID is a unique user identifier assigned to a specific user that consists of an alphanumeric string. The CID is stored in a first-party cookie on a user's computer, and it allows Qualtrics to track the respondent across web pages. The CID is associated with the user's account in Qualtrics, which allows Qualtrics to store the user's data.

63. The SIID is a unique user identifier assigned to a specific user that consists of an alphanumeric string. The SID is stored in a first-party cookie on a user's computer, and it allows Qualtrics to track the user and to associate the responses with their CID.

64. In addition to the above-identified unique user identifiers and/or cookies, Site Intercept also utilizes the following additional unique user identifiers and/or cookies associated with users of the Kaiser Website: (i) ZoneID and/or ZID; (ii) InterceptID; (iii) ActionSetID; and (iv) CreativeID (collectively the "Additional Qualtrics Identifiers"). A Kaiser Website user's ZoneID and/or ZID identifier or cookie is an alphanumeric string. A Kaiser Website user's InterceptID identifier and/or cookie is an alphanumeric string that has the same value as the user's SIID. A Kaiser Website user's ActionSetID identifier or cookie is an alphanumeric string that has the same value as the user's ASID. A Kaiser Website user's CreativeID is an alphanumeric string with the same value as the user's CID.

65. Site Intercept also collects and sends to Qualtrics identifying information about a user's web browser, which it collectively terms "User-Agent" ("User Agent Data").

66. As integrated into Kaiser Website, Site Intercept collects and sends to Qualtrics user data and identifying information, including PII and PHI, in three steps ("Qualtrics' Data Collection Process"). First, Site Intercept sends to Qualtrics' servers a user's ASID, CID, and SIID. Next, Site Intercept sends to Qualtrics' servers the additional user data described below, including a user's

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone: (206) 676-7000
Fax: (206) 676-7001

medical information, where it is combined with the user's ASID, CID, and SIID, along with the Additional Qualtrics Identifiers. Through this step, Qualtrics is able to link users to their medical information. Finally, Qualtrics' servers send a packet of digital data containing the user's unique user identifiers and medical data back to the user's internet browser. Through these steps of data transference, Qualtrics is able to match specific users to their medical information.

67. As integrated into the Kaiser Website, Site Intercept collects a plethora of Private Data, including PII and PHI, from Kaiser Members when they use the Kaiser Website without their knowledge or consent. The Private Data collected includes, as further described herein, search queries, visited webpages, videos, prescriptions, medical conditions, immunization records, and allergies.

68. **Search Queries**: The Kaiser website contains an integrated search bar that allows visitors to the Kaiser Website to search for information on Kaiser's Website using search terms, similar to using an Internet search engine like Google or Yahoo. Whenever a user on Kaiser's Website utilizes the search bar on Kaiser's Website to search for information, Site Intercept intercepts and collects the search terms entered by the user, along with unique user identifiers associated with the user, including ASID, CID, and SSID, through Qualtrics' Data Collection Process. The unique user identifiers allow Qualtrics to link the search terms to a specific user and identify the user. Qualtrics' ability to identify the user is enhanced by Site Intercept's collection of User Agent Data.

69. Site Intercept collects all search queries, without discerning their sensitivity, including, for example, those related to specific medical conditions a user is afflicted with, symptoms a user is experiencing, or medications a user is prescribed.

70. Kaiser Members, including Plaintiff and the Class Members, are unaware that Qualtrics is intercepting and collecting the above-described data through Site Intercept, and have not provided their consent, whether implied or express, for Qualtrics to obtain this data, for Kaiser to allow Qualtrics to obtain this data, or for Kaiser to share this data with Qualtrics.

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone: (206) 676-7000
Fax: (206) 676-7001

71. **Visited Webpages**: Site Intercept also intercepts and collects the URL (*i.e.,* web address) and/or title of each page on the Kaiser Website that a user navigates to and the unique user identifiers associated with the user, including ASID, CID, and SSID, through Qualtrics' Data Collection Process. The unique user identifiers allow Qualtrics to link the visited webpage to a specific user and identify the user. Qualtrics' ability to identify the user is enhanced by Site Intercept's collection of User Agent Data. The collection of a user's visited URLs and/or their titles occurs regardless of whether the user is logged into her Kaiser Account.

72. Furthermore, as explained below, when a Kaiser Member is logged into her Kaiser account, the collected URLs and webpage titles may divulge to Qualtrics a large swath of the user's medical history and PHI, including the medications a user is prescribed, the medical conditions a user suffers from, the user's immunization record, the user's allergies, and the results of a user's medical tests. Such URLs and page titles, when linked with unique user identifiers such as ASID, CID, and SSID, allow Qualtrics to link medical information, including PHI, to individual users.

73. Kaiser Website users, including Kaiser Members accessing their Kaiser Accounts through the Kaiser Website, such as Plaintiff and the Class Members, are unaware that Qualtrics is intercepting and collecting the above-described data through Site Intercept, and have not provided their consent, whether implied or express, for Qualtrics to obtain this data, for Kaiser to allow Qualtrics to obtain this data, or for Kaiser to share this data with Qualtrics.

74. **Videos**: The Kaiser Website contains various videos that are available for users to watch. When a user accesses a video on the Kaiser Website, Site Intercept intercepts and collects the URL of the webpage on which the video appears, along with unique user identifiers associated with the user, including ASID, CID, and SSID, through Qualtrics' Data Collection Process. The unique user identifiers allow Qualtrics to link the accessed video to a specific user and identify the user. Qualtrics' ability to identify the user is enhanced by Site Intercept's collection of User Agent Data. The interception and collection of data relating to videos on the Kaiser Website occurs regardless of whether the user is logged in to her Kaiser Account.

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone: (206) 676-7000
Fax: (206) 676-7001

75. Kaiser Members, including Plaintiff and the Class Members, are unaware that Qualtrics is intercepting and collecting the above-described data through Site Intercept, and have not provided their consent, whether implied or express, for Qualtrics to obtain this data, for Kaiser to allow Qualtrics to obtain this data, or for Kaiser to share this data with Qualtrics.

76. **Prescriptions**: When logged in to her Kaiser Account on the Kaiser Website, a Kaiser Member is able to view each of her prescribed medications by navigating to her personalized "Prescription Details" page. When viewing her list of medications, a Kaiser Member is able to click on a medication to navigate to a webpage within Kaiser's "Drug encyclopedia" with additional information about that medication in order to learn more about it. Unbeknownst to Kaiser Members, when a Kaiser Members clicks on a medication and navigates to that medication's "Drug encyclopedia" webpage, Site Intercept intercepts and collects: (i) the URL for that page, which includes the medication's reference number in Kaiser's "Drug encyclopedia" and sometimes the medication's name; and (ii) the user's ASID, CID, and SSID, through Qualtrics' Data Collection Process. The unique user identifiers allow Qualtrics to link the prescribed medication to a specific user, identify the user. Qualtrics' ability to identify the user is enhanced by Site Intercept's collection of User Agent Data.

77. The above-described data is PHI, since it is individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.

78. Kaiser Members, including Plaintiff and the Class Members, are unaware that Qualtrics is intercepting and collecting the above-described data through Site Intercept, and have not provided their consent, whether implied or express, for Qualtrics to obtain this data, for Kaiser to allow Qualtrics to obtain this data, or for Kaiser to share this data with Qualtrics.

79. **Medical Conditions**: When logged in to her Kaiser Account on the Kaiser Website, a Kaiser Member is able to view each of her medical conditions by navigating to her personalized "Medical Record" page and then further navigating to her personalized "Health summary" page.

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone: (206) 676-7000
Fax: (206) 676-7001

When viewing her list of medical conditions, each listed condition contains a hyperlink reading "Learn more" that, when clicked, automatically runs a search on the Kaiser Website for that medical condition using the name of the condition as a search query and navigates the Kaiser Member to a webpage on the Kaiser Website containing the search results. Unbeknownst to Kaiser Members, when a Kaiser Member clicks on the "Learn more" hyperlink for a given medical condition, Site Intercept intercepts and collects: the URL of the page containing the search results, which contains the name of the medical condition used for the search query and reveals that the user navigated from her personalized "Health Summary" subpage within her "Medical Record" page accessed from her Kaiser Account; and (ii) the user's ASID, CID, and SSID, through Qualtrics' Data Collection Process. The unique user identifiers allow Qualtrics to link the medical condition to a specific user and identify the user. Qualtrics' ability to identify the user is enhanced by Site Intercept's collection of User Agent Data. Additionally, since Site Intercept also intercepts and collects data showing that the user accessed the page containing the search results from her personalized "Health Summary" page, and from her personalized "Medical Record" page more generally, which are only accessible when the user logs in to her Kaiser Account, Qualtrics is aware that the user is a Kaiser Member, and that the user suffers from the medical condition.

80. The above-described data is PHI, since it is individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.

81. Kaiser Members, including Plaintiff and the Class Members, are unaware that Qualtrics is intercepting and collecting the above-described data through Site Intercept, and have not provided their consent, whether implied or express, for Qualtrics to obtain this data, for Kaiser to allow Qualtrics to obtain this data, or for Kaiser to share this data with Qualtrics.

82. **Immunization Record**: When logged in to her Kaiser Account on the Kaiser Website, a Kaiser Member is able to view each of her immunizations by navigating to her personalized "Medical Record" page, from there navigating to her personalized "Health summary"

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone: (206) 676-7000
Fax: (206) 676-7001

page, and then selecting the "Immunizations" tab. When viewing her list of immunizations, each listed immunization contains a hyperlink reading "Learn more" that, when clicked, automatically runs a search on the Kaiser Website for the immunization using the name of the immunization as a search query and navigates the Kaiser Member to a webpage on the Kaiser Website containing the search results. Unbeknownst to Kaiser Members, when a Kaiser Member clicks on the "Learn more" hyperlink for a given immunization, Site Intercept intercepts and collects: (i) the URL of the page containing the search results, which contains the name of the immunization used for the search query and reveals that the user navigated from her personalized "Medical Record" page accessed from her Kaiser Account; and (ii) the user's ASID, CID, and SSID, through Qualtrics' Data Collection Process. The unique user identifiers allow Qualtrics to link the immunization to a specific user and identify the user. Qualtrics' ability to identify the user is enhanced by Site Intercept's collection of User Agent Data. Additionally, since Site Intercept also intercepts and collects data showing that the user accessed the page containing the search results from her personalized "Medical Record" page, which is only accessible when the user logs in to her Kaiser Account, Qualtrics is aware that the user is a Kaiser Member, and that the user has received the immunization.

83. The above-described data is PHI, since it is individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.

84. Kaiser Members, including Plaintiff and the Class Members, are unaware that Qualtrics is intercepting and collecting the above-described data through Site Intercept, and have not provided their consent, whether implied or express, for Qualtrics to obtain this data, for Kaiser to allow Qualtrics to obtain this data, or for Kaiser to share this data with Qualtrics.

85. **Allergies**: When logged in to her Kaiser Account on the Kaiser Website, a Kaiser Member is able to view each of her allergies by navigating to her personalized "Medical Record" page, from there navigating to her personalized "Health summary" page, and then selecting the

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone: (206) 676-7000
Fax: (206) 676-7001

"Allergies" tab. When viewing her list of immunizations, each listed immunization contains a hyperlink reading "Learn more" that, when clicked, automatically runs a search on the Kaiser Website for the allergy using the name of the allergy as a search query and navigates the Kaiser Member to a webpage on the Kaiser Website containing the search results. Unbeknownst to Kaiser Members, when a Kaiser Member clicks on the "Learn more" hyperlink for a given allergy, Site Intercept intercepts and collects: (i) the URL of the page containing the search results, which contains the name of the allergy used for the search query and reveals that the user navigated from her personalized "Medical Record" page accessed from her Kaiser Account; and (ii) the user's ASID, CID, and SSID, through Qualtrics' Data Collection Process. The unique user identifiers allow Qualtrics to link the allergy to a specific user and identify the user. Qualtrics' ability to identify the user is enhanced by Site Intercept's collection of User Agent Data. Additionally, since Site Intercept also intercepts and collects showing that the user accessed the page containing the search results from her personalized "Medical Record" page, which is only accessible when the user logs in to her Kaiser Account, Qualtrics is aware that the user is a Kaiser Member, and that the user suffers from the allergy.

86. The above-described data is PHI, since it is individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.

87. Kaiser Members, including Plaintiff and the Class Members, are unaware that Qualtrics is intercepting and collecting the above-described data through Site Intercepts, and have not provided their consent, whether implied or express, for Qualtrics to obtain this data, for Kaiser to allow Qualtrics to obtain this data, or for Kaiser to share this data with Qualtrics.

D. Plaintiff' and the Class's PII Has Value

88. The value of personal data is well understood and generally accepted as a form of currency.

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone: (206) 676-7000
Fax: (206) 676-7001

89. It is by now incontrovertible that a robust market for this data undergirds the tech economy.

90. The robust market for user data has been analogized to the "oil" of the tech industry.[5] A 2015 article from TechCrunch accurately noted that "Data has become a strategic asset that allows companies to acquire or maintain a competitive edge."[6] That article noted that the value of a single Internet user—or really, a single user's data—varied from about $15 to more than $40.

91. The Organization for Economic Cooperation and Development ("OECD") itself has published numerous volumes discussing how to value data such as that which is the subject matter of this Complaint, including as early as 2013, with its publication "Exploring the Economic of Personal Data: A Survey of Methodologies for Measuring Monetary Value".[7] The OECD recognizes that data is a key competitive input not only in the digital economy but in all markets: "Big data now represents a core economic asset that can create significant competitive advantage for firms and drive innovation and growth."[8]

92. In *The Age of Surveillance Capitalism*, Harvard Business School Professor Shoshanna Zuboff notes that large corporations like Verizon, AT&T and Comcast have transformed their business models from fee-for-services-provided to monetizing their users' data—including user data that is not necessary for product or service use, which she refers to as "behavioral surplus."[9] In essence, Professor Zuboff explains that revenue from user data pervades every economic

---

[5] *The world's most valuable resource is no longer oil, but data*, The Economist (May 6, 2017). https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longeroil-but-data.

[6] Pauline Glickman and Nicolas Glady, *What's the Value of Your Data?* TechCrunch (Oct. 13, 2015), https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/.

[7] *Exploring the Economic of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD Digital Economy Paper No. 220 at 7 (Apr. 2, 2013), http://dx.doi.org/10.1787/5k486qtxldmq-en.

[8] *Supporting Investment in Knowledge Capital, Growth and Innovation*, OECD, at 319 (Oct. 13, 2013), https://www.oecd-ilibrary.org/industry-and-services/supporting-investment-in-knowledgecapital-growth-and-innovation_9789264193307-en.

[9] Shoshanna Zuboff, The Age of Surveillance Capitalism 166 (2019).

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone: (206) 676-7000
Fax: (206) 676-7001

transaction in the modern economy. It is a fundamental assumption of these revenues that there is a ***market*** for this data; data generated by Kaiser Members has economic value.

93. Professor Paul M. Schwartz writing in the Harvard Law Review, notes:

> Personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from the trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information.[10]

94. This economic value has been leveraged largely by corporations who pioneered the methods of its extraction, analysis, and use. However, the data also has economic value to users. Market exchanges have sprung up where individual users like Plaintiff herein can sell or monetize their own data. For example, Nielsen Data and Mobile Computer will pay users for their data.[11] Likewise, apps such as Zynn, a TikTok competitor, pay users to sign up and interact with the app.[12]

95. There are countless examples of this kind of market, which is growing more robust as information asymmetries are diminished through revelations to users as to how their data is being collected and used.

96. As Professors Acquisti, Taylor and Wagman relayed in their 2016 article "The Economics of Privacy," published in the Journal of Economic Literature:

> Such vast amounts of collected data have obvious and substantial economic value. Individuals' traits and attributes (such as a person's age, address, gender, income, preferences, and reservation prices, but also her clickthroughs, comments posted online, photos uploaded to social media, and so forth) are increasingly regarded as business

---

[10] Paul M. Schwartz, Property, Privacy, and Personal Data, 117 Harv. L. Rev. 2055, 2056-57 (2004).

[11] Kevin Mercandante, *Ten Apps for Selling Your Data for Cash*, Best Wallet Hacks (June 10, 2020), https://wallethacks.com/apps-for-selling-your-data/.

[12] Jacob Kastrenakes, *A New TikTok Clone hit the top of the App Store by Paying users to watch videos*, The Verge (May 29, 2020), https://www.theverge.com/2020/5/29/21274994/zynn-tiktokclone-pay-watch-videos-kuaishou-bytedance-rival.

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone: (206) 676-7000
Fax: (206) 676-7001

> assets that can be used to target services or offers, provide relevant advertising, or be traded with other parties.[13]

97. There is also a private market for users' personal information. One study by content marketing agency Fractl has found that an individual's online identity, including hacked financial accounts, can be sold for $1,200 on the dark web.[14] These rates are assumed to be discounted because they do not operate in competitive markets, but rather, in an illegal marketplace. If a criminal can sell other users' content, surely users can sell their own.

98. As to health data specifically, as detailed in an article in Canada's National Post:

> As part of the multibillion-dollar worldwide data brokerage industry, health data is one of the most sought-after commodities. De-identified data can be re identified and brazen decisions to release records with identifiable information are becoming commonplace).[15]

99. Further demonstrating the financial value of Class Members' ***medical data***, CNBC has reported that hospital executives have received a growing number of bids for user data:

> Hospitals, many of which are increasingly in dire financial straits, are weighing a lucrative new opportunity: selling patient health information to tech companies.
>
> Aaron Miri is chief information officer at Dell Medical School and University of Texas Health in Austin, so he gets plenty of tech start-ups approaching him to pitch deals and partnerships. Five years ago, he'd get about one pitch per quarter. But these days, with huge data-driven players like Amazon and Google making incursions into the health space, and venture money flooding into Silicon Valley start-ups aiming to bring machine learning to health care, the cadence is far more frequent.
>
> "It's all the time," he said via phone. "Often, once a day or more."

---

[13] Alessandro Acquisti, Curtis Taylor, and Liad Wagman, *The Economics of Privacy*, 54 J. of Econ. Literature 2, at 444 (June 2016), https://www.heinz.cmu.edu/~acquisti/papers/AcquistiTaylorWagman-JEL-2016.pdf.

[14] Maria LaMagna, *The sad truth about how much your Google data is worth on the dark web*, MarketWatch (June 6, 2018), https://www.marketwatch.com/story/spooked-by-the-Googleprivacy-violations-this-is-how-much-your-personal-data-is-worth-on-the-dark-web-2018-03-20.

[15] National Post, IRIS KULBATSKI: THE DANGERS OF ELECTRONIC HEALTH RECORDS, February 26, 2020, https://nationalpost.com/opinion/iris-kulbatski-the-dangers-of-electronichealth-records (last visited Dec. 29, 2022) (internal citations omitted).

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone: (206) 676-7000
Fax: (206) 676-7001

* * *

> [H]ealth systems administrators say [the data] could also be used in unintended or harmful ways, like being cross-referenced with other data to identify individuals at higher risk of diseases and then raise their health premiums, or to target advertising to individuals.[16]

100. The CNBC article also explained:

> De-identified patient data has become its own small economy: There's a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers. Just one company alone, IQVIA, said on its website that it has access to more than 600 million patient records globally that are nonidentified, much of which it accesses through provider organizations. The buyers, which include pharma marketers, will often use it for things like clinical trial recruiting
>
> But hospital execs worry that this data may be used in unintended ways, and not always in the patient's best interest.
>
> * * *
>
> Tech companies are also under particular scrutiny because they already have access to a massive trove of information about people, which they use to serve their own needs. For instance, the health data Google collects could eventually help it micro-target advertisements to people with particular health conditions. Policymakers are proactively calling for a revision and potential upgrade of the health privacy rules known as HIPAA, out of concern for what might happen as tech companies continue to march into the medical sector.[17]

101. Time Magazine similarly, in an article titled, HOW YOUR MEDICAL DATA FUELS A HIDDEN MULTI-BILLION DOLLAR INDUSTRY, referenced the "growth of the big health data bazaar," in which patients' health information is sold. It reported that:

> [T]the secondary market in information unrelated to a patient's direct treatment poses growing risks, privacy experts say. That's because clues in anonymized patient dossiers make it possible for outsiders to

---

[16] CNBC, HOSPITAL EXECS SAY THEY ARE GETTING FLOODED WITH REQUESTS FOR YOUR HEALTH DATA, https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-withrequests-for-your-health-data.html (last visited Dec. 29, 2022).

[17] *Id.*

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone: (206) 676-7000
Fax: (206) 676-7001

> determine your identity, especially as computing power advances in the future.[18]

102. In short, there is economic value to users' data. The exact number will be a matter for experts to determine.

103. Defendants have intercepted and collected Plaintiff's and Class Members' Private Data, including PHI and PII, without providing anything of value to Plaintiff and Class Members in exchange for that Private Data.

104. Defendants accessed Plaintiff's and the Class Members' Private Data, including PHI and PII, without permission. The unauthorized access to Plaintiff's and Class Members' Private Data, including PII and PHI, has diminished the value of that Private Data. Defendants have also failed to provide any consideration for that Private Data. These actions and omissions have resulted in harm to Plaintiff and Class Members.

E. Defendants Intercepted and Collected Plaintiff's Private Data, Including PII and PHI, Causing Plaintiff Harm

105. Plaintiff has been a Kaiser Member for at least 10 years and has used the Kaiser Website throughout her membership. She has an account on the Kaiser Website. While logged into that account, she used the search function; accessed immunization and medical records; made appointments; reviewed physician information; reviewed medical conditions; and watched videos. Defendants unlawfully intercepted and collected such data along with her personal identifiers. As a result of Defendants' actions, Plaintiff suffered harm.

V. TOLLING, CONCEALMENT, AND ESTOPPEL

106. Plaintiff repeats and incorporates all other paragraphs as if fully set forth herein.

107. The applicable statutes of limitations are tolled as a result of Defendants' knowing and active concealment of their conduct alleged above.

---

[18] Time, HOW YOUR MEDICAL DATA FUELS A HIDDEN MULTI-BILLION DOLLAR INDUSTRY, https://time.com/4588104/medical-data-industry/ (last visited Dec. 29, 2022).

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone: (206) 676-7000
Fax: (206) 676-7001

108. As alleged above, Plaintiff and Class Members did not know and could not have known when they used the Kaiser Website that the Defendants' SDKs were (and still are) implemented on the Kaiser Website and that Defendants' SDKs would collect and intercept Plaintiff's and the Class Members' Private Data, including PII and PHI. Plaintiff and the Class Members could not have discovered Defendants' unlawful conduct with reasonable due diligence.

109. Defendants' SDKs were secretly implemented on the Kaiser Website, and no indication was provided to Kaiser Members that their Private Data, including PII and PHI, would be collected and intercepted by Defendants' SDKs.

110. Defendants had exclusive and superior knowledge that Defendants' SDKs implemented on the Kaiser Website would collect and intercept Kaiser Members' personal information, including PII and PHI, yet failed to disclose to Kaiser Members that by interacting with the Kaiser Website their Private Data, including PII and PHI, would be collected and intercepted by Defendants.

111. Plaintiff and Class Members could not with due diligence have discovered the full scope of Defendants' conduct because the implementation of Defendants' SDKs on the Kaiser Website is highly technical and there were no disclosures or other indications by Kaiser or Defendants that would inform a reasonable consumer or user of the Kaiser Website that Defendants were collecting and intercepting the Private Data, including PII and PHI, of Kaiser Members.

112. The earliest Plaintiff and Class Members could have known about Defendants' conduct was shortly before the filing of this Complaint.

113. And when the action was filed, Defendants were under duty to disclose the true character, quality, and nature of their activities to Plaintiff and the Class Members. Defendants are therefore estopped from relying on any statute of limitations.

VI. CLASS ACTION ALLEGATIONS

114. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23(b)(1)(A) and/or 23(b)(3), individually and on behalf of the following Classes.

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone: (206) 676-7000
Fax: (206) 676-7001

First Nationwide Class: All natural persons residing in the United States who are current or former Kaiser Members and had their PHI taken by Defendants while using the Kaiser Website.

First California Subclass: All natural persons residing in California who are current or former Kaiser Members and had their PHI taken by Defendants while using the Kaiser Website.

Second Nationwide Class: All natural persons residing in the United States who are current or former Kaiser Members and had their Private Data, other than PHI, taken by Defendants while using the Kaiser Website.

Second California Subclass: All natural persons residing in California who are current or former Kaiser Members and had their Private Data, other than PHI, taken by Defendants while using the Kaiser Website.

115. **Numerosity**: The exact number of members of the Classes are unknown and unavailable to Plaintiff at this time, but individual joinder in this case is impracticable. The Classes likely consist of millions of individuals, and the members can be identified through Defendants' records.

116. **Predominant Common Questions**: The Classes' claims present common questions of law and fact, and those questions predominate over any questions that may affect individual Class Members. Common questions for the Classes include, but are not limited to, the following:

(a) Whether Defendants collected Plaintiff and Class Members' Private Data, including PHI and PII, when they used the Kaiser Website;

(b) Whether Defendants' acts and practices violated the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq.*;

(c) Whether Defendants' acts and practices violated California's Constitution, Art. 1, § 1;

(d) Whether Defendants' acts and practices violated Class Members' common law privacy rights and/or intruded upon their seclusion;

(e) Whether Defendants acts and practices violated the Computer Fraud and Abuse Act, 18 U.S.C. §§ 1030, *et seq.*;

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone: (206) 676-7000
Fax: (206) 676-7001

(f) Whether Defendants were unjustly enriched;

(g) Whether Defendants' acts and practices violated California's Business and Professions Code §§ 17200, *et seq.*;

(h) Whether Defendants' acts and practices violated California Penal Code § 496(a) and (c);

(i) Whether Defendants' acts and practices constitute conversion under California law;

117. **Typicality**: Plaintiff's claims are typical of the claims of the other members of the Class. The claims of Plaintiff and the members of the Class arise from the same conduct by Defendant and are based on the same legal theories. Defendant acted or refused to act on grounds generally applicable to the class, and Defendant's policies and practices challenged herein apply equally and uniformly to each class member, including Plaintiff.

118. **Adequate Representation**: Plaintiff has and will continue to fairly and adequately represent and protect the interests of the Class. Plaintiff has retained counsel competent and experienced in complex litigation and class actions, including litigations to remedy privacy violations. Plaintiff has no interest that is antagonistic to the interests of the Class, and Defendant has no defenses unique to any Plaintiff. Plaintiff and her counsel are committed to vigorously prosecuting this action on behalf of the members of the Class, and they have the resources to do so. Neither Plaintiff nor her counsel have any interest adverse to the interests of the other members of the Class.

119. **Substantial Benefits**: This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone: (206) 676-7000
Fax: (206) 676-7001

adjudication, economies of scale, and comprehensive supervision by a single court.[19] Class treatment will create economies of time, effort, and expense and promote uniform decision-making.

120. A class action is a particularly efficient and appropriate procedure in this case because absent a class action Defendant would gain an unconscionable economic advantage. Individual plaintiffs have limited resources and could be outspent many times over by Defendant. Moreover, the recovery in each individual suit would not cover the cost of litigation.

121. Defendant's course of conduct described herein is common to each Class Member; maintaining individual actions would create a risk of inconsistent results.

122. Plaintiff reserves the right to revise the foregoing class allegations and definitions based on facts learned and legal developments following additional investigation, discovery, or otherwise.

VII. CALIFORNIA LAW APPLIES TO THE ENTIRE CLASS

123. California substantive law applies to every member of the Class. California substantive law may be constitutionally applied to the claims of Plaintiff and the Classes under the Due Process Clause, 14th Amend. § 1, and the Full Faith and Credit Clause, Art. IV. § 1 of the U.S. Constitution. California has significant contact, or significant aggregation of contacts, to the claims asserted by Plaintiff and Class Members, thereby creating state interests to ensure that the choice of California state law is not arbitrary or unfair.

124. Defendant Microsoft's principal executive offices are located at One Microsoft Way, Redmond, Washington 98052. Microsoft also maintains several offices in California and conducts substantial business in California, such that California has an interest in regulating Microsoft's conduct under its laws. Microsoft's decision to have offices in California and avail itself of

[19] As to Fed. R. Civ. Proc. 23(b)(3)(B), Plaintiff acknowledges that a case concerning the use of SDKs on the Kaiser Website was recently filed in the U.S. District Court for the Northern District of California, captioned *Doe v. Kaiser Foundation Health Plan, Inc., et al.*, Case No. 4:23-cv-02207-DMR. However, that action is brought on behalf of putative classes different from those defined herein, and that action does not name Microsoft or Qualtrics as defendants.

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone: (206) 676-7000
Fax: (206) 676-7001

California's laws renders the application of California law to the claims herein constitutionally permissible.

125. Defendant Qualtrics' co-headquarters are located at 1201 2nd Ave., Suite 2700, Seattle, Washington 98101 and at 333 West River Park Drive, Provo, Utah 64604. Qualtrics also maintains an office in Palo Alto, California and conducts substantial business in California, such that California has an interest in regulating Qualtrics' conduct under its laws. Qualtrics' decision to have offices in California and avail itself of California's laws renders the application of California law to the claims herein constitutionally permissible.

126. The application of California law to the Class is also appropriate under Washington's choice of law rules because California has significant contacts to the claims of Plaintiff and the proposed Classes, and California has a greater interest in applying its laws here than any other interested state.

VIII CLAIMS FOR RELIEF

FIRST CLAIM FOR RELIEF
Violation of the California Invasion of Privacy Act
Cal. Penal Code §§ 630, 631, et seq. ("CIPA")
(On Behalf of Plaintiff, the Classes, and the Subclasses Against All Defendants)

127. Plaintiff, Class Members, and Subclass Members re-allege and incorporate the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

128. Defendants violated CIPA by intentionally reading or attempting to read, and/or learning the contents of the online communications between (i) Plaintiff, Class Members and Subclass Members, on the one hand, and (ii) the Kaiser Website, on the other, without Plaintiff, Class Members, and Subclass Members' consent. These online communications include, but are not limited to, Plaintiff, Class Members, and Subclass Members' Private Data, including PHI and PII. Such data includes, among other items, search queries, medical conditions, videos, webpages visited, prescriptions, immunization records, allergies, and doctor searches.

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone: (206) 676-7000
Fax: (206) 676-7001

129. The California Legislature enacted CIPA finding that "advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society." Cal. Penal Code § 630. Thus, the intent behind CIPA is "to protect the right of privacy of the people of this state." *Id.*

130. Cal. Penal Code § 631(a) provides a remedy against "[a]ny person who, by means of any machine, instrument, or contrivance, or in any other manner, intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, or who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section."

131. Defendants violated § 631(a) by intercepting, storing, reading, attempting to read, attempting to learn, using, and attempting to use Plaintiff, the Class Members, and the Subclass Members' Private Data, including PHI and PII, without "the consent of all parties," while the same was in transit or passing over any wire, line, or cable, or was being sent from, or received at any place within California.

132. Unbeknownst to Plaintiff, the Class Members and the Subclass Members, the Kaiser Website contains Defendants' SDKs, which intercept, collect, and use the Private Data, including

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone: (206) 676-7000
Fax: (206) 676-7001

PHI and PII. Such data includes, among other items, search queries, medical conditions, videos, webpages visited, prescriptions, immunization records, allergies, and doctor searches.

133. The Private Data, including the PHI and PII, is individually identifiable health information and other sensitive information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in other form or medium.

134. Plaintiff, Class Members, and Subclass Members' Private Data, including their PHI and PII, has economic value.

135. Because Plaintiff, Class Members, and Subclass Members are unaware that Defendants are intercepting, collecting, and using their Private Data, including PHI and PII, through Defendants' SDKs, Plaintiff, Class Members, and Subclass Members could not have consented to the interception, collection, and use of their Private Data, including PHI and PII, by Defendants.

136. On information and belief, Defendants' interception, collection, and use of Plaintiff, Class Members, and Subclass Members' Private Data, including PHI and PII, is knowing and intentional.

137. The information communicated between Plaintiff, Class Members, and Subclass Members, on the one hand, and Kaiser's Website, on the other, was transmitted to and/or from the state of California.

138. Plaintiff, Class Members, and Subclass Members seek statutory damages in accordance with § 637.2(a), which provides that any person who has been injured by a violation of this chapter (including § 632) may bring an action for the greater of: (1) $5,000 per violation; or (2) three times the amount of damages sustained by Plaintiff, the Class Members, and the Subclass Members, in an amount to be proven at trial, as well as injunctive or other equitable relief. Plaintiff, Class Members, and Subclass Members are therefore entitled to at least $5,000 per violation.

139. Section 637.2(b) provides that any person may "bring an action to enjoin and restrain any violation of this chapter." Plaintiff, Class Members, and Subclass Members further seek injunctive relief, as they have suffered irreparable injury from Defendants' misconduct. Plaintiff,

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone: (206) 676-7000
Fax: (206) 676-7001

Class Members, and Subclass Members' Private Data, including personal, private, and sensitive medical information, has been intercepted, collected, viewed, read, learned, accessed, stored, used, and transmitted by Defendants, and has not been destroyed, and due to the continuing threat of such injury, Plaintiffs, Class Members, and Subclass Members have no adequate remedy at law.

SECOND CLAIM FOR RELIEF
Violation of the California Invasion of Privacy Act
Cal. Penal Code §§ 632, *et seq.* ("CIPA")
(On Behalf of Plaintiff, the Classes, and the Subclasses Against All Defendants)

140. Plaintiff, Class Members, and Subclass Members re-allege and incorporate the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

141. Defendants violated CIPA by using their SDKs and receiving servers (where the data is saved and recorded) which are recording devices under CIPA, to eavesdrop upon the confidential communications between Plaintiff, Class Members, and Subclass Members, on the one hand, and Kaiser's Website, on the other.

142. Cal. Penal Code § 632 prohibits use of "a recording device to eavesdrop upon or record [a] confidential communication" without consent of all parties to the communication. For the purposes of the statute, 'confidential communication' means a communication carried on in circumstances that may reasonably indicate a participant wishes the communication be confined to the parties thereto. *Id.* § 632(c).

143. Defendants violated Cal. Penal Code § 632 by intercepting, accessing, recording, eavesdropping, and transmitting Plaintiff, Class Members, and Subclass Members' Private Data, including sensitive medical information, communicated with the Kaiser Website through searches and clicks on that website.

144. Unbeknownst to Plaintiff, Class Members and Subclass Members, the Kaiser Website contains Defendants' SDKs that intercept, collect, and use Plaintiff, Class Members, and Subclass Members' Private Data, including PHI and PII. Such data includes, among other items,

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone: (206) 676-7000
Fax: (206) 676-7001

search queries, medical conditions, videos, webpages visited, prescriptions, immunization records, allergies, and doctor searches.

145. The Private Data, including PHI and PII, is individually identifiable health information and other sensitive information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in other form or medium.

146. Plaintiff, Class Members, and Subclass Members' Private Data, including PHI and PII, has economic value.

147. Because Plaintiff, Class Members, and Subclass Members are unaware that Defendants are collecting their Private Data, including PHI and PII, through Defendants' SDKs, Plaintiff, Class Members, and Subclass Members could not have consented to the interception, collection, and use of Plaintiff, Class Members, and Subclass Members' Private Data, including PHI and PII, by Defendants.

148. On information and belief, Defendants' interception, collection, and use of Plaintiff, Class Members, and Subclass Members' Private Data, including PHI and PII, is knowing and intentional.

149. Plaintiff, Class Members, and Subclass Members seek statutory damages in accordance with § 637.2(a), which provides that any person who has been injured by a violation of this chapter (including § 632) may bring an action for the greater of: (1) $5,000 per violation; or (2) three times the amount of damages sustained by Plaintiff, Class Members, and Subclass Members, in an amount to be proven at trial, as well as injunctive or other equitable relief. Plaintiff, Class Members, and Subclass Members are therefore entitled to at least $5,000 per violation.

150. Section 637.2(b) provides that any person may "bring an action to enjoin and restrain any violation of this chapter." Plaintiff, Class Members, and Subclass Members further seek injunctive relief, as they have suffered irreparable injury from Defendants' misconduct. Plaintiff, Class Members, and Subclass Members' Private Data, including personal, private, and sensitive medical information, has been intercepted, collected, viewed, read, learned, accessed, stored, used,

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone: (206) 676-7000
Fax: (206) 676-7001

and transmitted by Defendants, and has not been destroyed, and due to the continuing threat of such injury, Plaintiffs, Class Members, and Subclass Members have no adequate remedy at law.

THIRD CLAIM FOR RELIEF
Violation of the Right to Privacy – California Constitution
(On Behalf of Plaintiff, the Classes, and the Subclasses Against All Defendants)

151. Plaintiff, Class Members, and Subclass Members re-allege and incorporate the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

152. Defendants violated Article I of the California Constitution by intercepting, reading, collecting, and using Plaintiff, Class Members, and Subclass Members' Private Data, including PHI and PII, without Plaintiff, Class Members, and Subclass Members' consent.

153. The California Constitution expressly provides for a right to privacy: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring possessing and protecting property, and pursuing and obtaining safety, happiness and privacy." Cal. Const., art. I § 1.

154. Plaintiff, Class Members, and Subclass Members have a legally protected privacy interest in their Private Data, including PHI and PII, that Defendants have intercepted, collected, and used.

155. Plaintiff, Class Members, and Subclass Members have a reasonable expectation of privacy concerning their Private Data, including PHI and PII, under the circumstances.

156. The reasonableness of Plaintiff, Class Members, and Subclass Members' expectations of privacy are supported by the clandestine nature of Defendants' taking of Plaintiff, Class Members, and Subclass Members' Private Data, including PHI and PII. Defendants acted with disregard for Plaintiff, Class Members, and Subclass Members' privacy.

157. Defendants' conduct violated Plaintiff, Class Members, and Subclass Members' privacy interests, is highly offensive to a reasonable person, and constitutes an egregious breach of social norms. Defendants intentionally violated Plaintiff, Class Members, and Subclass Members'

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone: (206) 676-7000
Fax: (206) 676-7001

privacy interests by intentionally designing their SDKs to surreptitiously intercept, collect, and use Plaintiff, Class Members, and Subclass Members' Private Data, including PHI and PII.

158. Defendants' intrusions are highly offensive to a reasonable person, as evidenced by substantial research, literature, and governmental enforcement and investigative efforts to protect consumer privacy against surreptitious technological intrusions.

159. Plaintiff, Class Members, and Subclass Members were harmed by the intrusions.

160. Defendants' conduct was a substantial factor in causing the harm suffered by Plaintiff, Class Members, and Subclass Members.

161. Plaintiff, Class Members, and Subclass Members seek actual, nominal and punitive damages as a result of Defendants' actions. Punitive damages are warranted because Defendants' malicious, oppressive, and willful actions were calculated to injure Plaintiff, Class Members, and Subclass Members, and were made in conscious disregard of Plaintiff, Class Members, and Subclass Members' rights. Punitive damages are also warranted to deter Defendants from engaging in future misconduct.

162. Plaintiff, Class Members, and Subclass Members seek restitution and disgorgement for Defendants' violation of their privacy rights. A person acting in conscious disregard for the rights of another must disgorge all profit because disgorgement both benefits the injured parties and deters the perpetrator from committing the same unlawful actions again. Disgorgement is available for conduct that constitutes "conscious interference with a claimant's legally protected interests," including tortious conduct or conduct that violates another duty or prohibition. Restatement (3rd) of Restitution and Unjust Enrichment, §§ 40, 44.

FOURTH CLAIM FOR RELIEF
Invasion of Privacy/Intrusion Upon Seclusion
(On Behalf of Plaintiff, the Classes, and the Subclasses Against All Defendants)

163. Plaintiff, Class Members, and Subclass Members re-allege and incorporate the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone: (206) 676-7000
Fax: (206) 676-7001

164. Defendants violated Plaintiff, Class Members, and Subclass Members' common law privacy rights by intercepting, reading, collecting, and using Plaintiff, Class Members, and Subclass Members' Private Data, including PHI and PII, without Plaintiff, Class Members, and Subclass Members' consent.

165. Defendants' interception, collection, and use of this Private Data, including PHI and PII, without consent is highly offensive to a reasonable person, and caused harm to Plaintiff, Class Members, and Subclass Members.

166. Plaintiff, Class Members, and Subclass Members have a legally protected privacy interest in the Private Data, including PHI and PII.

167. Plaintiff, Class Members, and Subclass Members reasonably expected their Private Data, including PHI and PII, would remain private, and would not be intercepted, collected, or used for any improper purpose or by any unauthorized parties.

168. Unbeknownst to Plaintiff, Class Members, and Subclass Members, the Kaiser Website contains Defendants' SDKs that intercept, collect, and use Plaintiff, Class Members, and Subclass Members' Private Data, including PHI and PII. Such data includes, among other items, search queries, medical conditions, videos, webpages visited, prescriptions, immunization records, allergies, and doctor searches.

169. The Private Data, including PHI and PII, is individually identifiable health information and other sensitive information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in other form or medium.

170. Plaintiff, Class Members, and Subclass Members' Private Data, including PHI and PII, has economic value.

171. Because Plaintiff, Class Members, and Subclass Members are unaware that Defendants are intercepting, collecting, and using their Private Data, including PHI and PII, through Defendants' SDKs, Plaintiff, Class Members, and Subclass Members could not have consented to the interception, collection, and use of their Private Data, including PHI and PII, by Defendants.

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone: (206) 676-7000
Fax: (206) 676-7001

172. On information and belief, Defendants' interception, collection, and use of Plaintiff, Class Members, and Subclass Members' Private Data, including PHI and PII, is knowing and intentional.

173. Defendants violated Plaintiff, Class Members, and Subclass Members' privacy rights by intercepting, collecting and using such Private Data, including PHI and PII, in an unauthorized manner.

174. Defendants did these acts without the consent of Plaintiff, Class Members, and Subclass Members, and with reckless disregard for their privacy rights.

175. Defendants violated Plaintiff, Class Members, and Subclass Members' privacy rights guaranteed under California law, including under Article 1 Section 1 of the California Constitution and California common law.

176. Defendants' unlawful invasions of Plaintiff, Class Members, and Subclass Members' Private Data, including PHI and PII, intruded upon and frustrated Plaintiff, Class Member, and Subclass Members' reasonable expectations of privacy. This conduct directly and proximately caused Plaintiff, Class Members, and Subclass Members' injuries.

177. Plaintiff, Class Members, and Subclass Members are entitled to actual and punitive damages, and injunctive relief.

FIFTH CLAIM FOR RELIEF
Violation of the Computer Fraud and Abuse Act ("CFAA")
18 U.S.C. § 1030, *et seq.*
(On Behalf of Plaintiff, the Classes, and the Subclasses Against All Defendants)

178. Plaintiff, Class Members, and Subclass Members re-allege and incorporate the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

179. Plaintiff, Class Members, and Subclass Members' computer devices are, and at all relevant times were, used for interstate communication and commerce and are therefore "protected computers" under 18 U.S.C. § 1030(e)(2)(B).

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone: (206) 676-7000
Fax: (206) 676-7001

180. Defendants intentionally accessed Plaintiff, Class Members, and Subclass Members protected computers and obtained information thereby, and in doing so exceeded any authority granted by Plaintiffs, Class Members, and Subclass Members to access the protected computers in violation of 18 U.S.C. § 1030(a)(2), (a)(2)(C). Plaintiff, Class Members, and Subclass Members have a civil cause of action for violation of the CFAA under 18 U.S.C. § 1030(g) and have suffered damage or loss.

181. Defendants violated the CFAA by intercepting, reading, collecting, and using Plaintiff, Class Members, and Subclass Members' Private Data, including PHI and PII, without Plaintiff, Class Members, and Subclass Members' consent.

182. Defendants' conduct caused "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value" under 18 U.S.C. § 1030(c)(4)(A)(i)(I) because the unauthorized access and collection of data caused a diminution in value of Plaintiff, Class Members, and Subclass Members' Private Data, including PHI and PII, both of which occurred to millions of Class members, easily aggregating at least $5,000 in value.

183. The interception, collection, transmission, and use of the Private Data, including PHI and PII, constitutes "a threat to public health or safety" under 18 U.S.C. § 1030(c)(4)(A)(i)(IV).

184. Plaintiff, Class Members, and Subclass Members are therefore entitled to "maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." 18 U.S.C. § 1030(g).

SIXTH CLAIM FOR RELIEF
Unjust Enrichment.
(On Behalf of Plaintiff, the Classes, and the Subclasses Against All Defendants)

185. Plaintiff, Class Members, and Subclass Members re-allege and incorporate the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

186. Plaintiff, Class Members, and Subclass Members have conferred substantial benefits on Defendants by virtue of their use of the Kaiser Website. These benefits include Defendants' interception, collection, and use of Plaintiff, Class Members, and Subclass Members' Private Data,

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone: (206) 676-7000
Fax: (206) 676-7001

including PHI and PII, and the revenues and profits resulting from targeted advertising and other uses of such data by Defendants.

187. Defendants have knowingly and willingly accepted and enjoyed these benefits.

188. Defendants either knew or should have known that the benefits conferred by Plaintiff, Class Members, and Subclass Members were given and received with the expectation that Defendants would not intercept, collect, and use the Private Data, including PHI and PII, that Defendants have intercepted, collected, and used without Plaintiff, Class Members, and Subclass Members' consent. For Defendants to retain those benefits under these circumstances is inequitable.

189. Through deliberate violation of Plaintiff, Class Members, and Subclass Members' privacy interests and statutory and constitutional rights, Defendants reaped benefits that led to each Defendant wrongfully receiving profits.

190. Equity demands disgorgement of Defendants' ill-gotten gains. Defendants will be unjustly enriched unless they are ordered to disgorge those profits for the benefit of Plaintiff, Class Members, and Subclass Members.

191. As a direct and proximate result of Defendants' wrongful conduct and unjust enrichment, Plaintiff, Class Members, and Subclass Members are entitled to restitution from Defendants and the institution of a constructive trust disgorging all profits, benefits, and other compensation obtained by Defendants through this inequitable conduct.

SEVENTH CLAIM FOR RELIEF
Violation of the California Unfair Competition Law
Cal. Bus. & Prof. Code § 17200, *et seq.*
(On Behalf of Plaintiff, the Classes, and the Subclasses Against All Defendants)

192. Plaintiff, Class Members, and Subclass Members re-allege and incorporate the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

193. California's Unfair Competition Law ("UCL") prohibits any "unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." Cal. Bus. & Prof. Code § 17200.

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone: (206) 676-7000
Fax: (206) 676-7001

194. Defendants engaged in unfair and unlawful business practices by intercepting, collecting, viewing, accessing, storing, improperly using, and transmitting Plaintiff, Class Members, and Subclass Members' Private Data, including PHI and PII, in violation of the UCL.

195. Without the consent of Plaintiff, Class Members, and Subclass Members, Defendants intercepted, collected, and used this Private Data, including PHI and PII, for unauthorized purposes. Defendants failed to meet legal and industry standards for protection of Plaintiff, Class Members, and Subclass Members' Private Data, including PHI and PII.

196. The acts and omissions of Defendants constitute "business practices" within the meaning of the UCL.

197. The Private Data, including PHI and PII, is individually identifiable health information and other sensitive information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in other form or medium.

198. Plaintiff, Class Members, and Subclass Members' Private Data, including PHI and PII, has economic value.

199. Because Plaintiff, Class Members, and Subclass Members are unaware that Defendants are intercepting, collecting, and using their Private Data, including PHI and PII, through Defendants' SDKs, Plaintiff, Class Members, and Subclass Members could not have consented to the interception, collection, and use of their Private Data, including PHI and PII, by Defendants.

200. On information and belief, Defendants' collection of Plaintiff, Class Members, and Subclass Members' Private Data, including PHI and PII, is knowing and intentional.

201. Defendants violated the unlawful prong of the UCL by violating Plaintiff, Class Members, and Subclass Members' constitutional rights to privacy, and state and federal privacy statutes including the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq.*; the Computer Fraud and Abuse Act, 18 U.S.C. §§ 1030, *et seq.*; and California Penal Code § 496(a) and (c).

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone: (206) 676-7000
Fax: (206) 676-7001

202. Defendants violated the unfair prong of the UCL because their acts, omissions and conduct contravened the well-established public policy interest in securing consumers' privacy in and control over their personally identifiable information, as well as the well-established public policy interest in securing medical patients' privacy in and control over their private medical and health information. These interests are clearly articulated in the above referenced statutes. Defendants' conduct was immoral, unethical, oppressive and unscrupulous, and caused substantial injury, including to Plaintiff, Class Members, and Subclass Members.

203. The harm caused by Defendants conduct outweighs any potential benefits derived from such conduct. Moreover, there were reasonably available alternatives to this conduct that would have allowed Defendants to achieve any legitimate business interest.

204. As a result of Defendants' violations of the UCL, Plaintiff, Class Members, and Subclass Members have suffered injury in fact, including lost consideration for provision of access to their Private Data, including PHI and PII, and diminished value of that data.

205. Alternatively, Plaintiff, Class Members, and Subclass Members are entitled to equitable relief to restore them to the position they would have been in had Defendants not engaged in unfair and unlawful competition, and to prevent future privacy invasions. Plaintiff, Class Members, and Subclass Members are entitled to an injunction, restitution, and disgorgement of all profits gained as a result of Defendants' unlawful and unfair practices.

EIGHTH CLAIM FOR RELIEF
Violation of the California Penal Code § 496(a) and (c) – Statutory Larceny
(On Behalf of Plaintiff, the Classes, and the Subclasses Against All Defendants)

206. Plaintiff, Class Members, and Subclass Members re-allege and incorporate the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

207. Pursuant to California Penal Code Section 484, "[e]very person who shall feloniously steal, take, carry, lead, or drive away the personal property of another, . . . is guilty of theft."

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone: (206) 676-7000
Fax: (206) 676-7001

208. Under California law, Plaintiff, Class Members, and Subclass Members' Private Data, including PHI and PII, constitutes property that may be the subject of theft. See Calhoun v. Google LLC, 526 F. Supp. 3d 605 (N.D. Cal. 2021).

209. Defendants surreptitiously intercepted, collected, used, and exercised dominion and control over Plaintiff, Class Members, and Subclass Members' Private Data, including PHI and PII, through Defendants' SDKs, thereby constituting theft. Such data includes, among other items, search queries, medical conditions, videos, webpages visited, prescriptions, immunization records, allergies, and doctor searches.

210. Defendants knew that this data was obtained in a manner constituting theft.

NINTH CLAIM FOR RELIEF
Conversion
(On Behalf of Plaintiff, the Classes, and the Subclasses Against All Defendants)

211. Plaintiff, Class Members, and Subclass Members re-allege and incorporate the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

212. Property is the right of any person to possess, use, enjoy, or dispose of a thing, including intangible things such as data or communications. Under California law, Plaintiff, Class Members, and Subclass Members' Private Data, including PHI and PII, constitutes property that may be the subject of theft. *See Calhoun v. Google LLC*, 526 F. Supp. 3d 605 (N.D. Cal. 2021).

213. Defendants unlawfully intercepted, collected, used, and exercised dominion and control over Plaintiff, Class Members, and Subclass Members' Private Data, including PHI and PII, without authorization.

214. Defendants wrongfully exercised dominion and control over Plaintiff, Class Members, and Subclass Members' Private Data, including PHI and PII, and have not returned it.

215. Plaintiff, Class Members, and Subclass Members have been damaged as a result of Defendants' unlawful conversion of their property.

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone: (206) 676-7000
Fax: (206) 676-7001

PRAYER OF RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all others similarly situated, requests that this Court:

A. Certify the Classes and Subclasses as a class action pursuant to Federal Rule of Civil Procedure Rule 23, designate Plaintiff as the Class Representative and name the undersigned as Class Counsel;

B. Award compensatory damages, including all applicable statutory damages, for damages caused by Defendants' wrongdoing;

C. Award punitive damages to deter Defendants from committing similar wrongdoing in the future;

D. Permanently enjoin Defendants from intercepting, collecting, and using the Private Data, including PHI and PII, without consent;

E. Order Defendants to destroy the Private Data, including PHI and PII, in their possession;

F. Award pre-judgment interest to Plaintiff, Class Members, and Subclass Members to the fullest extent allowed by law;

G. Award Plaintiff, Class Members, and Subclass Members the costs of bringing this action, including the payment of reasonable attorneys' fees and administrative and litigation costs and expenses; and

H. Grant such other relief as the Court deems just and proper.

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone: (206) 676-7000
Fax: (206) 676-7001

DATED this 15th day of May, 2023.

Respectfully submitted,

SUMMIT LAW GROUP, PLLC

By *s/ Alexander A. Baehr*

Alexander A. Baehr, WSBA No. 25320
315 Fifth Avenue S, Suite 1000
Seattle, WA 98104
Telephone: (206) 676-7000
Email: alexb@summitlaw.com

BIRD, MARELLA, BOXER, WOLPERT, NESSIM, DROOKS, LINCENBERG & RHOW, PC

Ekwan E. Rhow (pro hac vice forthcoming)
Marc E. Masters (pro hac vice forthcoming)
Barr Benyamin (pro hac vice forthcoming)
1875 Century Park East, 23rd Floor
Los Angeles, California 90067
Telephone: (310) 201-2100
Email: erhow@birdmarella.com
mmasters@birdmarella.com
bbenyamin@birdmarella.com

GLANCY PRONGAY & MURRAY LLP

Jonathan Rotter (pro hac vice forthcoming)
Kara M. Wolke (pro hac vice forthcoming)
Pavithra Rajesh (pro hac vice forthcoming)
1925 Century Park East, Suite 2100
Los Angeles, California 90067
Telephone: (310) 201-9150
Facsimile: (310) 201-9160
Email: jrotter@glancylaw.com
kwolke@glancylaw.com
prajesh@glancylaw.com

Counsel for Plaintiff